UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/922,041	08/03/2001	Larry H. Gass	ITL.0506US (P10475)	7270

21906 7590 07/20/2006

TROP PRUNER & HU, PC
1616 S. VOSS ROAD, SUITE 750
HOUSTON, TX 77057-2631

EXAMINER	
NGUYEN, MINH DIEU T	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/922,041	GASS ET AL.	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 April 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

4a) Of the above claim(s) *2,8-12,14,18,20,22-26,28,30,31 and 35* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 3-7, 13, 15-17, 19, 21, 27, 29, 32-34, 36-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the communication dated April 25, 2006.

Claims 1, 3-7, 13, 15-17, 19, 21, 27, 29, 32-34 and 36-42 are pending.

Response to Arguments

2. Applicant's arguments filed April 25, 2006 have been fully considered but they are not persuasive. Applicant argues as to claims 33 and 40, the citation does not talk about firmware, firmware having two different portions, one is upgradable and the other is not and providing information for authenticating an upgrade of the second portion. The claimed limitations are addressed clearly in the Abstract (i.e. upgrading device firmware using a certificate system), paragraph [0076] meets the limitation of firmware having two different portions, one is upgradable (i.e. semi-permanent) and the other is not upgradable (i.e. permanent and non-modifiable), paragraphs [0099] and [0248] address providing information for authenticating an upgrade of the second portion. As to claim 1, the applicant argues that Sudia does not teach retrieving a second public key, examiner contends that Sudia discloses multiple instruction keys of the trusted third parties in the device firmware besides manufacturer's signature key, if the manufacturer's key is compromised, lost or destroyed (i.e. key is not valid), then the trusted third party's instruction key can be used to replace, so the replacement key is viewed as the second key or backup key (claim 13). The limitations in claim 19 are addressed in part by the admitted information in the specification "a hardware

initialization portion; an operating system loader portion" (page 1, lines 15-19) and in part by Falik (see addressed claim 13 in the previous office action page 5). Falik discloses locking a device storing the firmware program such that a second portion of the firmware program is not readable (Falik, paragraph [0015]).

Claim Objections

3. Claim 35 is objected because it depends on canceled claim 31.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 33 and 40 are rejected under 35 U.S.C. 102(e) as being anticipated by Sudia (2001/0050990).

Sudia discloses a method comprising providing a first portion of a firmware code which is not upgradable (i.e. permanent and non-modifiable); providing a second portion of a firmware code that is upgradable (semi-permanent and modifiable) (paragraph [0076]); and providing information for authenticating (paragraphs [0099], [0248]) an upgrade of the second portion in the first portion.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 3, 5-7, 13, 15-17, 21, 27 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Angelo et al. (5,748,940) in view of Falik et al. (2002/0166061) and further in view of Sudia (2001/0050990).

a) As to claims 1 and 27, Angelo discloses a secure updating of non-volatile memory comprising identifying a firmware upgrade request by a firmware program (i.e. a flash bit set to indicate a flash update will occur, col. 3, lines 3-6); retrieving a file signed with a private key (Fig. 3, element 310); validating a file with a public key (Fig. 3, element 312; col. 3, lines 39-52); upgrading a portion of the firmware program by the firmware program (Fig. 3, element 316).

Angelo does not disclose locking a device storing the firmware program such that a second portion of the firmware program is not readable.

Falik discloses an apparatus and method for protecting the contents of a shared memory in a memory device comprising a step of locking a device storing the firmware program such that a second portion of the firmware program is not readable (page 2, paragraph [0015]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of locking device storing the firmware program such that a

second portion of the firmware program is not readable in the system of Angelo as Falik teaches so as to prevent access to the firmware by unauthorized users.

Angelo and Falik do not disclose the steps of validating the public key and retrieving a second public key from the firmware program if the public key is not valid.

Sudia discloses a cryptographic system and method for upgrading device firmware (Abstract) of a trusted device comprising validating the public key and retrieving a second public key from the firmware program if the public key is not valid (page 22, paragraph [0251]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of validating the public key and retrieving a second public key from the firmware program if the public key is not valid in the system of Angelo and Falik as Sudia teaches so as to efficiently perform firmware upgrade request.

b) As to claim 3, Angelo as modified above discloses identifying a firmware upgrade request by a firmware program further comprising reading a flag, wherein the flag is located in a non-volatile medium (Fig. 1, element 120; i.e. flash bit) and determining that the flag is set (col. 2, lines 6-8).

c) As to claims 5 and 29, Falik as modified above discloses locking flags is utilized to implement software protection for each flash memory device blocks (page 1, paragraph [0014]; i.e. determining that the file is not authentic and locking the device).

d) As to claim 6, Falik as modified above discloses locking the device after upgrading a portion of the firmware program by the firmware program (page 9, paragraph [0111]; page 11, paragraph [0122]).

e) As to claim 13, Angelo discloses a secure updating of non-volatile memory comprising identifying a firmware upgrade request by a firmware program (i.e. a flash bit set to indicate a flash update will occur, col. 3, lines 3-6); retrieving a file signed with a private key (Fig. 3, element 310); validating a file with a public key (Fig. 3, element 312; col. 3, lines 39-52); upgrading a portion of the firmware program by the firmware program (Fig. 3, element 316).

Angelo does not disclose locking a device storing the firmware program such that a second portion of the firmware program is not readable.

Falik discloses an apparatus and method for protecting the contents of a shared memory in a memory device comprising a step of locking a device storing the firmware program such that a second portion of the firmware program is not readable (page 2, paragraph [0015]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of locking device storing the firmware program such that a second portion of the firmware program is not readable in the system of Angelo as Falik teaches so as to prevent access to the firmware by unauthorized users.

Angelo discloses the firmware program comprising a second portion further including a minimal boot portion (Fig. 3, element 306); a signature authentication portion (Fig. 3, element 312) and a write device portion (Fig. 3, element 316).

Angelo and Falik do not disclose the steps of validating the public key and retrieving a second public key from the firmware program if the public key is not valid.

Sudia discloses a cryptographic system and method for upgrading device firmware (Abstract) of a trusted device comprising the firmware program first portion including the public key and a backup public key (page 22, paragraph [0251]) and the firmware program second portion including a minimal boot portion; a signature authentication portion and a write device portion (paragraphs [0097-0101]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of including a first portion with public key and a backup public key and a second portion with a minimal boot portion; a signature authentication portion and a write device portion in the firmware program in the system of Angelo and Falik as Sudia teaches so as to efficiently upgrading or replacing trusted firmware code routines (paragraph [0083]).

f) As to claim 7, Angelo as modified above discloses the second portion of the firmware program is a public key (col. 3, lines 39-52).

g) As to claim 15, Angelo as modified above discloses the firmware program further clears the upgrade flag (col. 2, line 8).

h) As to claim 16, Angelo as modified above discloses a persistent storage, wherein the file is located in the persistent storage (col. 2, lines 56-59).

i) As to claim 17, Falik as modified above discloses a network interface for connecting the system to a network, wherein the file is retrieved from the network (page 6, paragraph [0063]).

j) As to claim 21, Falik as modified above discloses the device is a flash memory (page 6, paragraph [0063]).

8. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Angelo et al. (5,748,940) in view of Falik et al. (2002/0166061) in view of Sudia (2001/0050990) and further in view of admitted information in the specification.

Angelo, Falik and Sudia do not disclose the portion of the firmware program further comprising a hardware initialization portion, an operating system loader portion. However Falik discloses locking a device storing the firmware program such that a second portion of the firmware program is not readable (page 2, paragraph [0015]).

The admitted information from the specification indicates firmware program comprises a hardware initialization portion and an operating system loader portion (page 1, lines 15-19).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having a portion of the firmware program further comprising a hardware initialization portion, an operating system loader portion and a device lock-out portion in the system of Angelo, Falik and Sudia so as to protect boot information from unauthorized tampering.

9. Claims 4 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Angelo et al. (5,748,940) in view of Falik et al. (2002/0166061) in view of Sudia (2001/0050990) and further in view of Toft (2002/0138592).

a) As to claim 32, Angelo discloses a secure updating of non-volatile memory comprising identifying a firmware upgrade request by a firmware program (i.e. a flash bit set to indicate a flash update will occur, col. 3, lines 3-6); retrieving a file signed with a

private key (Fig. 3, element 310); validating a file with a public key (Fig. 3, element 312; col. 3, lines 39-52); upgrading a portion of the firmware program by the firmware program (Fig. 3, element 316).

Angelo discloses identifying a firmware upgrade request by a firmware program further comprising reading a flag, wherein the flag is located in a non-volatile medium (Fig. 1, element 120; i.e. flash bit) and determining that the flag is set (col. 2, lines 6-8).

Angelo does not disclose locking a device storing the firmware program such that a second portion of the firmware program is not readable.

Falik discloses an apparatus and method for protecting the contents of a shared memory in a memory device comprising a step of locking a device storing the firmware program such that a second portion of the firmware program is not readable (page 2, paragraph [0015]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of locking device storing the firmware program such that a second portion of the firmware program is not readable in the system of Angelo as Falik teaches so as to prevent access to the firmware by unauthorized users.

Angelo and Falik do not disclose the steps of validating the public key and retrieving a second public key from the firmware program if the public key is not valid.

Sudia discloses a cryptographic system and method for upgrading device firmware (Abstract) of a trusted device comprising validating the public key and retrieving a second public key from the firmware program if the public key is not valid (page 22, paragraph [0251.

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of validating the public key and retrieving a second public key from the firmware program if the public key is not valid in the system of Angelo and Falik as Sudia teaches so as to efficiently perform firmware upgrade request.

Angelo, Falik and Sudia do not explicitly disclose the steps of deleting the file and clearing the flag.

Toft discloses clearing the update flag before rebooting the system (paragraph[0022]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of clearing the update flag in the system of Angelo, Falik and Sudia asToft teaches so as to properly control the update process.

Angelo, Falik, Sudia and Toft do not explicitly disclose deleting the file.

The examiner takes official notice that deleting the upgrade file after it is being used is a common practice to save system memory.

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of deleting the file in the system of Angelo, Falik, Sudia and Toft so as to save system memory.

b) As to claim 4, please see addressed above claim 32.

10. Claims 34-39 and 41-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia (2001/0050990) in view of Falik et al. (2002/0166061).

a) As to claim 34, Sudia does not disclose locking a first portion to prevent reading the first portion.

Falik discloses an apparatus and method for protecting the contents of a shared memory in a memory device comprising a step of locking a first portion to prevent reading the first portion (page 2, paragraph [0015]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of locking a first portion to prevent reading the first portion in the system of Sudia as Falik teaches so as to prevent access to the firmware by unauthorized users.

b) As to claims 35-37 and 41-42, Sudia discloses providing a signature authentication in the first portion (paragraph [0099]); providing two public keys (paragraphs [0087-0088]); providing two identical public keys (paragraphs [0088],[0094]).

c) As to claim 38, Sudia discloses providing instruction in the first portion to confirm the validity of a firmware upgrade file (paragraph [0248]).

d) As to claim 39, Falik discloses determining whether an upgrade request is authentic and if the upgrade request is not authentic, locking the first portion against being written (page 1, paragraph [0014]; i.e. determining that the file is not authentic and locking the device).

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

mdn
7/17/06

KAMBIZ ZAND
PRIMARY EXAMINER